UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,061	09/05/2003	David S. Colvin	COL404PUS	2060

			EXAMINER
36547	7590	12/05/2006	REVAK, CHRISTOPHER A

BIR LAW, PLC
13092 GLASGOW CT.
PLYMOUTH, MI 48170-5241

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
	10/605,061	COLVIN, DAVID S.
Office Action Summary	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>18 September 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-99</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-99</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>25 June 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>9/18/06</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1.   The information disclosure statement (IDS) submitted on September 18, 2006 is

in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is

considering the information disclosure statement.

Terminal Disclaimer

2.   The terminal disclaimer filed on September 18, 2006 disclaiming the terminal

portion of any patent granted on this application has been reviewed and is accepted.

The terminal disclaimer has been recorded.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-99 have been considered but are

moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-99 rejected under 35 U.S.C. 103(a) as being unpatentable over

Ananda, U.S. Patent 5,495,411 in view of Garceau et al, "General Controls in a Local

Area Network".

As per claim 1, Ananda teaches of a method for securing software to reduce

unauthorized use, the method comprising providing at least one hardware based

authorized representative entity installed on or in a user device; obtaining registration

information corresponding to at least one user device; generating an authentication

code at least partially based on the registration information; associating the

authentication code with the software; determining whether a current user device is

authorized based on the authentication code associated with the software and

registration information associated with the current user device; and controlling access

to the software based on whether the current user device is authorized (col. 3, lines 11-

15 & 21-28; col. 4, lines 18-28; and col. 11, lines 9-13). The teachings of Ananda

disclose of a continuous connection to the remote authorized representative entity and

fail to teach that the continuous connection to a remote authorized entity is not required.

It is disclosed by Garceau et al the user is required to contact a LAN administrator to

establish a new password when the maximum interval has expired for the password

being valid (see the top of page 3). The examiner notes that Garceau et al does not

require the user to be continuously connected with the LAN administrator and that the

user is required to contact the LAN administrator, it is a non-continuous connection with

the administrator, and the system can be shut down requiring the user to contact the

administrator prior to logging in again (see the top of page 3). It would have been

obvious to a person of ordinary skill in the art at the time of the invention to have been

motivated to apply repeated authentication intervals without being continuously

connected with an administrator. The teachings of Garceau et al recite motivation for

applying this requirement by disclosing that total control is given to the administrator to

ensure that the passwords are regularly changed and that the password values are

random (see the top of page 3). It is obvious that the teachings of Ananda would have

been made more secure by requiring contact with an administrator at certain periods of

time to ensure that the passwords are changed and that the password values are

random through a non-continuous connection with the administrator as is taught by

Garceau et al.

As per claim 2, Ananda discloses wherein the software is self-activating and self-

authenticating in conjunction with the hardware based authorized representative located

on or in the user device (col. 10, lines 4-15).

As per claim 3, it is taught by Ananda wherein the software comprises data

representing content selected from the group consisting of music, video, an application

program, an operating system component, a game, a movie, graphics, watermarked

works, a magazine, and a book (col. 1, lines 17-19).

As per claim 4, it is disclosed by Ananda wherein the step of obtaining

registration information is at least partially performed by the at least one hardware

based authorized representative entity installed on or in the user device (col. 3, lines 21-

29).

As per claim 5, it is taught by Ananda wherein the step of generating an authentication code is at least partially performed by the at least one hardware based authorized representative entity installed on or in the user device (col. 4, lines 39-46).

As per claim 6, Ananda teaches wherein the step of obtaining registration information is performed by a remotely located authorized representative entity (col. 1, lines 17-19 and col. 11, lines 61-65).

As per claim 7, Ananda discloses wherein the step of generating an authentication code is performed by a remotely located authorized representative entity (col. 11, lines 9-13).

As per claim 8, it is taught by Ananda wherein the steps of obtaining, generating, associating, determining, and controlling are at least partially performed by a resident hardware based authorized representative entity installed on at least one user device (col. 10, lines 4-15 and col. 11, lines 61-65).

As per claim 9, it is disclosed by Ananda wherein registration information associated with the current user device remains within a trusted network associated with the user device (col. 3, lines 16-29).

As per claim 10, Ananda teaches wherein registration information associated with the current user device is not communicated to any third party (col. 3, lines 16-29).

As per claim 11, Ananda discloses wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed prior to transferring the software to the current user device (col. 3, lines 16-49).

As per claim 12, it is taught by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed substantially concurrently with transferring the software to the current user device (col. 3, lines 16-49 and col. 4, lines 39-48).

As per claim 13, it is disclosed by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed following transferring the software to the current user device (col. 3, lines 16-49 and col. 10, lines 8-15).

As per claim 14, Ananda teaches wherein the steps of obtaining, generating, and associating are performed by a remote authorized representative entity (col. 10, lines 8-15).

As per claim 15, Ananda discloses wherein the hardware based authorized representative functions are hard coded (col. 9, line 57 through col. 10, line 3).

As per claim 16, it is taught by Ananda wherein the hardware based authorized representative functions are programmable (col. 9, line 57 through col. 10, line 3).

As per claim 17, it is disclosed by Ananda wherein the hardware based authorized representative functions are both hard coded and programmable (col. 9, line 57 through col. 10, line 3).

As per claim 18, Ananda teaches wherein the hardware device is a computer chip (col. 6, lines 57-63).

As per claim 19, Ananda discloses wherein the hardware device is integral with a CPU (col. 6, lines 57-63).

As per claim 20, it is taught by Ananda wherein the hardware device is a PC card (col. 6, lines 57-63).

As per claim 21, it is disclosed by Ananda wherein the hardware device is a microprocessor (col. 6, lines 57-63).

As per claim 22, Ananda teaches wherein the steps of determining whether a current user device is authorized and controlling access to the software are at least partially performed by the hardware based authorized representative entity installed on or in a user device (col. 10, lines 4-15 and col. 11, lines 61-65).

As per claim 23, Ananda discloses wherein the software is electronically distributed (col. 9, lines 35-36).

As per claim 24, it is taught by Ananda wherein the software is transferred to a user device from a computer readable storage medium (col. 6, lines 57-63 and col. 9, lines 35-36).

As per claim 25, it is disclosed by Ananda wherein at least one authentication code is distributed with the software (col. 3, lines 11-15).

As per claim 26, Ananda teaches wherein the authentication code corresponds to a group of user devices (col. 3, lines 11-15).

As per claim 27, Ananda discloses wherein the authentication code at least partially corresponds to a manufacturer of a user device (col. 9, lines 5-6).

As per claim 28, it is taught by Ananda wherein the authentication code at least partially corresponds to a model of a user device (col. 9, lines 5-6).

As per claim 29, Ananda teaches wherein the authentication code at least partially corresponds to a unique user device (col. 3, lines 11-15).

As per claim 30, Ananda discloses wherein the steps of determining whether a current user device is authorized and controlling access to the software are performed by a remotely located authorized representative entity (col. 3, lines 16-49).

As per claim 31, it is taught by Ananda wherein the step of controlling access to the software comprises preventing transfer of at least a portion of the software to the current user device (col. 3, lines 16-49).

As per claim 32, it is disclosed by Ananda wherein the step of controlling access to the software comprises preventing the current user device from utilizing the software (col. 10, lines 13-15).

As per claim 33, Ananda teaches wherein the steps of determining and controlling are at least partially performed by an authorized representative installed on a secondary user device (col. 10, lines 4-15).

As per claim 34, Ananda discloses wherein the steps of obtaining, generating, and associating are performed by a primary user device and the steps of determining and controlling are performed by a secondary user device (col. 10, lines 4-15).

As per claim 35, it is taught by Ananda of further comprising encrypting the authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 36, it is disclosed by Ananda of further comprising encrypting the registration information (col. 9, lines 25-34).

As per claim 37, Ananda teaches of further comprising associating an identifier with the software to trigger authentication by an authorized representative entity (col. 10, lines 63 through col. 11, line 15).

As per claim 38, Ananda discloses of further comprising securing any means for generating the authentication code after generating the authentication code associated with the software (col. 10, line 63 through col. 11, line 15).

As per claim 39, it is taught by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are at least partially performed by a hardware based authorized representative entity installed on or in a user device, the method further comprising: modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software (col. 10, lines 8-15).

As per claim 40, it is disclosed by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by a remote authorized representative prior to distribution of the software (col. 3, lines 16-49).

As per claim 41, Ananda teaches of a method for securing software to reduce unauthorized use having an hardware based authorized representative entity installed on or in a user device, the method comprising determining whether the user device is authorized to access the software using the authorized representative entity; and controlling access to the software based on whether the user device is determined to be authorized (col. 3, lines 11-15 & 21-28; col. 4, lines 18-28; and col. 11, lines 9-13). The

teachings of Ananda disclose of a continuous connection to the remote authorized representative entity and fail to teach that the continuous connection to a remote authorized entity is not required. It is disclosed by Garceau et al the user is required to contact a LAN administrator to establish a new password when the maximum interval has expired for the password being valid (see the top of page 3). The examiner notes that Garceau et al does not require the user to be continuously connected with the LAN administrator and that the user is required to contact the LAN administrator, it is a non-continuous connection with the administrator, and the system can be shut down requiring the user to contact the administrator prior to logging in again (see the top of page 3). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply repeated authentication intervals without being continuously connected with an administrator. The teachings of Garceau et al recite motivation for applying this requirement by disclosing that total control is given to the administrator to ensure that the passwords are regularly changed and that the password values are random (see the top of page 3). It is obvious that the teachings of Ananda would have been made more secure by requiring contact with an administrator at certain periods of time to ensure that the passwords are changed and that the password values are random through a non-continuous connection with the administrator as is taught by Garceau et al.

As per claim 42, Ananda discloses wherein the software is self-authenticating in conjunction with the authorized representative located on or in the user device (col. 10, lines 4-15).

As per claim 43, it is taught by Ananda of further comprising determining whether the user device is authorized to access the software using a remotely located authorized representative entity in combination with the authorized representative entity installed on or in the user device (col. 10, lines 4-15 and col. 11, lines 61-65).

As per claim 44, it is disclosed by Ananda wherein the hardware based authorized representative functions are hard coded (col. 9, line 57 through col. 10, line 3).

As per claim 45, Ananda discloses wherein the hardware based authorized representative functions are programmable (col. 9, line 57 through col. 10, line 3).

As per claim 46, Ananda teaches wherein the hardware based authorized representative functions are both hard coded and programmable (col. 9, line 57 through col. 10, line 3).

As per claim 47, Ananda discloses wherein the hardware based authorized representative entity comprises a computer chip (col. 6, lines 57-63).

As per claim 48, it is taught by Ananda wherein the hardware based authorized representative entity is integral with the CPU (col. 6, lines 57-63).

As per claim 49, it is disclosed by Ananda wherein the hardware based authorized representative entity comprises a PC card (col. 6, lines 57-63).

As per claim 50, Ananda teaches wherein the hardware based authorized representative entity comprises program instructions executed by a microprocessor (col. 6, lines 57-63).

As per claim 51, Ananda discloses wherein the step of determining whether the user device is authorized comprises: comparing registration information associated with the user device to registration information associated with the software (col. 3, lines 16-49).

As per claim 52, it is taught by Ananda wherein the registration information associated with the software is embedded within an authentication code (col. 3, lines 24-28).

As per claim 53, it is disclosed by Ananda wherein the registration information associated with the software is encrypted (col. 11, line 61 through col. 12, line 14).

As per claim 54, Ananda teaches wherein the registration information includes hardware information (col. 9, lines 5-6).

As per claim 55, Ananda discloses wherein the registration information includes hardware information associated with a unique user device (col. 3, line 11-15).

As per claim 56, it is taught by Ananda wherein the hardware information includes a serial number (col. 8, lines 18-23).

As per claim 57, Ananda teaches wherein the registration information includes hardware information associated with a group of user devices (col. 3, lines 11-15).

As per claim 58, Ananda discloses wherein the hardware based authorized representative entity is installed by a manufacturer of the user device (col. 9, lines 35-36).

As per claim 59, it is taught by Ananda wherein the hardware based authorized representative entity is installed from a computer readable storage medium (col. 6, lines 57-63 and col. 9, lines 35-36).

As per claim 60, it is disclosed by Ananda wherein the hardware based authorized representative entity is downloaded to the user device (col. 9, lines 35-36).

As per claim 61, Ananda teaches wherein the authorized representative entity is transferred to the user device from a network (col. 9, lines 35-36).

As per claim 62, Ananda discloses wherein the step of controlling access comprises preventing the software from being transferred to a second user device (col. 10, lines 8-15).

As per claim 63, it is taught by Ananda wherein the step of controlling access comprises preventing the software from being executed by the user device (col. 10, lines 8-15).

As per claim 64, it is disclosed by Ananda wherein the step of controlling access comprises providing limited access to the software (col. 10, lines 8-15).

As per claim 65, Ananda teaches wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book (col. 1, lines 17-19).

As per claim 66, Ananda discloses wherein the software comprises instructions for generating at least one authentication code at least partially based on registration information associated with the user device (col. 11, lines 9-13).

As per claim 67, it is taught by Ananda wherein the software comprises instructions for encrypting the authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 68, it is disclosed by Ananda wherein the step of determining whether the user device is authorized comprises contacting a remote authorized representative entity if the authorized representative entity installed on or in a user device is unable to determine whether the user device is authorized (col. 10, lines 8-15).

As per claim 69, Ananda teaches wherein the step of determining whether the user device is authorized comprises contacting a remote authorized representative if the authorized representative entity installed on or in a user device determines that the user device is not authorized (col. 10, lines 8-15).

As per claim 70, Ananda discloses wherein the step of determining whether the user device is authorized comprises obtaining registration information associated with the user device and comparing the registration information associated with the user device with registration information encoded in an authentication code associated with the software (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 71, it is taught by Ananda of further comprising detecting an identifier associated with the software to trigger authentication functions performed by the hardware based authorized representative entity installed on or in the user device; and performing the steps of determining whether the user device is authorized and controlling access to the software only if the identifier is detected (col. 10, lines 8-15).

As per claim 72, it is disclosed by Ananda of further comprising automatically contacting a remote authorized representative based upon a triggering event to receive information (col. 4, line 61 through col. 5, line 10).

As per claim 73, Ananda teaches wherein the information is selected from a group consisting of updates, upgrades, patches, marketing information, promotional information, quality assurance information, network monitoring and metering information, and error and usage information (col. 20, lines 53-62).

As per claim 74, Ananda discloses wherein the information updates the authorized representative entity installed on or in the user device (col. 20, lines 53-62).

As per claim 75, it is taught by Ananda wherein the information modifies the software (col. 10, lines 8-15 and col. 20, lines 53-62).

As per claim 76, it is disclosed by Ananda wherein the triggering event is based on a user action (col. 3, lines 21-28).

As per claim 77, Ananda teaches wherein the automatic contact with the remote authorized representative is repeated (col. 10, lines 8-15).

As per claim 78, Ananda discloses of a method for reducing unauthorized use of software, the method comprising associating at least one identifier with the software corresponding to a request for digital rights management; distributing the software to a user; detecting the at least one identifier using an authorized representative entity; associating at least one authentication code with the software; determining whether a user device is authorized to access the software; and controlling access to the software based on whether the user device is authorized (col. 3, lines 11-15 & 21-28; col. 4, lines

18-28; and col. 11, lines 9-13). The teachings of Ananda disclose of a continuous connection to the remote authorized representative entity and fail to teach that the continuous connection to a remote authorized entity is not required. It is disclosed by Garceau et al the user is required to contact a LAN administrator to establish a new password when the maximum interval has expired for the password being valid (see the top of page 3). The examiner notes that Garceau et al does not require the user to be continuously connected with the LAN administrator and that the user is required to contact the LAN administrator, it is a non-continuous connection with the administrator, and the system can be shut down requiring the user to contact the administrator prior to logging in again (see the top of page 3). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply repeated authentication intervals without being continuously connected with an administrator. The teachings of Garceau et al recite motivation for applying this requirement by disclosing that total control is given to the administrator to ensure that the passwords are regularly changed and that the password values are random (see the top of page 3). It is obvious that the teachings of Ananda would have been made more secure by requiring contact with an administrator at certain periods of time to ensure that the passwords are changed and that the password values are random through a non-continuous connection with the administrator as is taught by Garceau et al.

As per claim 79, it is taught by Ananda wherein the software is self-activating and self-authenticating in conjunction with a hardware based authorized representative located on or in the user device (col. 10, lines 4-15).

As per claim 80, it is disclosed by Ananda of further comprising encrypting the at least one authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 81, Ananda teaches of further comprising obtaining registration information associated with at least one user device; and generating the at least one authentication code at least partially based on the registration information (col. 3, lines 21-28).

As per claim 82, Ananda discloses of further comprising encrypting the registration information (col. 11, line 61 through col. 12, line 14).

As per claim 83, it is taught by Ananda wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed before the step of distributing the software (col. 3, lines 11-31).

As per claim 84, it is disclosed by Ananda wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed substantially concurrently with the step of distributing the software (col. 3, lines 11-31).

As per claim 85, Ananda teaches wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed subsequent to the step of distributing the software (col. 3, lines 11-31).

As per claim 86, Ananda discloses wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed by an authorized representative entity installed on or in the user device (col. 3, lines 11-31; col. 10, lines 4-15; and col. 11, lines 61-65).

As per claim 87, Ananda teaches wherein the step of generating the at least one authentication code is performed by an authorized representative entity installed on or in the user device, the method further comprising securing the authentication code to resist user tampering (col. 11, lines 9-13).

As per claim 88, Ananda discloses wherein the step of securing comprises preventing the authorized representative entity installed on or in the user device from generating any more authentication codes for the software (col. 10, lines 4-15 and col. 11, lines 61-65).

As per claim 89, it is taught by Ananda wherein the step of securing comprises encrypting the authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 90, it is disclosed by Ananda of further comprising: determining whether an operational authorized representative entity is available locally; installing an authorized representative entity on or in the user device if an operational authorized representative entity is not available locally (col. 10, lines 4-15 and col. 11, lines 61-65).

As per claim 91, Ananda teaches wherein the step of installing comprises transferring the authorized representative entity to the user device from a remote authorized representative entity (col. 10, lines 4-15 and col. 11, lines 61-65).

As per claim 92, Ananda discloses wherein the step of installing comprises transferring the authorized representative entity to the user device from a computer readable storage medium (col. 6, lines 57-63 and col. 9, lines 35-36).

As per claim 93, it is taught by Ananda wherein the software includes an authorized representative entity and wherein the step of installing comprises transferring the authorized representative entity to the user device from the software (col. 6, lines 57-63 and col. 9, lines 35-36).

As per claim 94, it is disclosed by Ananda of further comprising determining whether an operational authorized representative entity is installed on or in the user device; and contacting a remote authorized representative entity if no operational authorized representative entity is installed on or in the user device (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 95, Ananda teaches wherein the remote authorized representative entity performs the steps of determining whether a user device is authorized and controlling access to the software (col. 10, lines 8-15).

As per claim 96, Ananda discloses of further comprising obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed prior to the step of distributing the software to a user (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 97, it is taught by Ananda of further comprising obtaining registration information including hardware specific information associated with a user

device, wherein the steps of obtaining registration information and associating at least

one authentication code are performed substantially concurrently with the step of

distributing the software to a user (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 98, it is disclosed by Ananda of further comprising obtaining

registration information including hardware specific information associated with a user

device, wherein the steps of obtaining registration information and associating at least

one authentication code are performed following the step of distributing the software to

a user (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 99, Ananda teaches wherein the step of controlling access to the

software comprises preventing the software from being transferred to the user device if

the user device is not authorized (col. 10, lines 8-15).

Conclusion

6.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Christopher A. Revak whose telephone number is 571-

272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CR

November 26, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER